JACOB M. HEATH (SBN 238959)
jheath@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025-1015
Telephone: +1 650 614 7400
Facsimile: +1 650 614 7401

THOMAS FU (SBN 325209)
tfu@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
777 South Figueroa Street, Suite 3200
Los Angeles, CA 90017-5855
Telephone: +1 213 629 2020
Facsimile: +1 213 612 2499

ARAVIND SWAMINATHAN (admitted *pro hac vice*)
aswaminathan@orrick.com
NICOLE M. TADANO (admitted *pro hac vice*)
ntadano@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
701 5th Avenue, Suite 5600
Seattle, WA 98104-7097
Telephone: +1 206 839 4300
Facsimile: +1 206 839 4301

Attorneys for Defendants,
Shopify Inc. and Shopify (USA) Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

Brandon Briskin, on behalf of himself and those similarly situated, Plaintiffs, v. Shopify Inc. and Shopify (USA) Inc., Defendants.	Case No. 4:21-cv-06269 **DEFENDANT SHOPIFY INC.'S MOTION TO DISMISS PLAINTIFF'S FIRST AMENDED CLASS ACTION COMPLAINT** Date: February 3, 2022 Time: 1:30 p.m. Location: Courtroom 3, 3rd Floor 1301 Clay Street Oakland, California Judge: The Honorable Phyllis J. Hamilton

NOTICE OF MOTION TO DISMISS

PLEASE TAKE NOTICE that on February 3, 2022 at 1:30 p.m., or as soon thereafter as the matter may be heard in Courtroom 3 (3rd Floor) of the above-entitled court, located at 1301 Clay Street, Oakland, California 94612, defendant Shopify Inc. will, and hereby does, move the Court under Federal Rules of Civil Procedure 8, 12(b)(2) and 12(b)(6) for an order dismissing the First Amended Class Action Complaint ("FAC") (ECF No. 17) of Plaintiff Brandon Briskin. This motion is based on this notice, the concurrently filed memorandum of points and authorities, and all other facts the court may or should take notice of, all files, records, and proceedings in this case, and any oral argument the Court may entertain.

STATEMENT OF RELIEF SOUGHT (CIVIL L.R. 7-2(B)(3)). Shopify Inc. seeks an Order pursuant to Federal Rule of Civil Procedure 8(a)(2) for failure to provide adequate notice of the claims against it, or in the alternative, pursuant to Federal Rule 12(b)(2) for lack of personal jurisdiction, or in the further alternative, Federal Rule of Civil Procedure 12(b)(6) dismissing the FAC for failure to state a claim upon which relief can be granted.

Dated: December 8, 2021 ORRICK, HERRINGTON & SUTCLIFFE LLP

By: */s/ Jacob M. Heath*
JACOB M. HEATH
THOMAS FU
Attorneys for Defendants
Shopify (USA), Inc. and Shopify Inc.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Other Authorities

The First Amended Complaint ("FAC") alleges that routine processing of commercial transactions on the internet is a crime. Several, in fact. When a customer pays with a credit card—whether in a physical store or online—the payment information is typically sent to a payment processor (not processed by the merchant), and then in turn to other entities. The FAC asserts, however, that because Plaintiff's credit card information for an online transaction was transmitted to Shopify Inc. for processing, rather than directly to the merchant who sold him athletic apparel, Shopify Inc. violated California's Constitution, various statutes, and the common law.

Those claims fail for at least four reasons. First, as explained in detail in Shopify (USA) Inc.'s MTD Brief, the FAC fails to distinguish between—and hence to provide adequate notice to—the separate entities Shopify Inc. and Shopify (USA) Inc. ("Shopify USA").[1] Second, this Court lacks personal jurisdiction over Shopify Inc. Third, Plaintiff's consent to the complained-of acts is fatal to all of his claims as pled. Despite his protestations that he was wholly unaware that his information would be transmitted to Shopify Inc., the webpages the FAC features prominently disclose that fact. And fourth, each claim independently fails to state a claim for relief on the merits: **Penal Code § 631** does not apply, because the FAC does not allege that Shopify Inc. "taps" or learns the "contents" of any communication, but that it processes purely transactional data for its merchants at their request. **Penal Code § 635** does not apply, because the FAC does not allege that Shopify Inc. manufactured a "device" "primarily" for eavesdropping, but rather software to conduct lawful sales transactions. No **right to privacy** is at issue here because the FAC does not allege an "egregious breach of the social norms," but rather standard commercial transactions. **Penal Code § 502** does not apply, because the FAC does not allege that Shopify Inc. overcame any code-based barrier to access a computer, but rather that it used routine cookies that are fully disclosed and easily prevented or deleted by those who wish to do so. The **Unfair Competition Law** does not apply for similar reasons: the FAC alleges only that Shopify Inc. engaged in standard

[1] Because the FAC's allegations fail to differentiate between Shopify Inc. and Shopify USA as required by Rule 8, *see infra* § IV.A, this motion treats its references to "Shopify" as "Shopify Inc." solely for the purpose of this motion where necessary to explain why the FAC fails under Rule 12(b)(6). Shopify Inc.'s and Shopify USA's arguments under Rules 8 and 12(b)(6) therefore mirror one another, and dismissal under either rule as to one entity necessitates dismissal as to the other. *See infra* § IV.C; *see also* Shopify USA MTD Br. § IV.C.

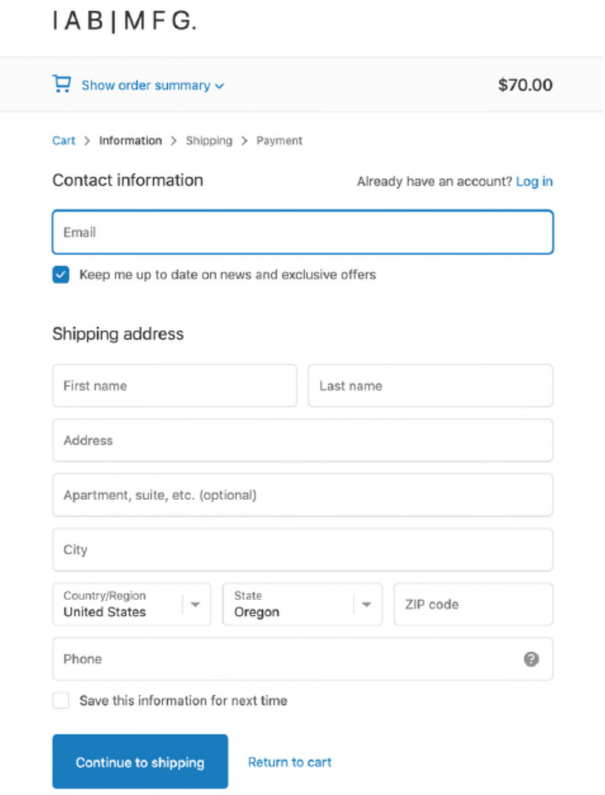
commercial transactions, the details of which are disclosed to the consumer in full, which are not unlawful, unfair, or fraudulent. And the **right of publicity** is not implicated, because the FAC fails to allege that Shopify Inc. makes use of Plaintiff's name or likeness. The FAC should be dismissed.

I. STATEMENT OF ISSUES TO BE DECIDED (CIVIL L.R. 7-4(a)(3))

Shopify Inc. seeks Rule 8 dismissal for failure to plead facts showing that Shopify Inc. caused Plaintiff's alleged harm, Rule 12(b)(2) dismissal for lack of personal jurisdiction, and Rule 12(b)(6) dismissal for failure to state a claim.

II. SUMMARY OF RELEVANT FACTS

The FAC alleges that in June 2019, Plaintiff purchased fitness apparel from Shopify Inc. merchant IABMFG through its website. FAC ¶ 50. In the course of that purchase, the FAC alleges Plaintiff was presented with the checkout screen reproduced at FAC ¶ 21 (**Fig. 1**). FAC ¶ 51. In providing these reproductions of IABMFG's current website, the FAC incorporates those webpages by reference, and the Court is permitted to consider their full context. *See Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005).



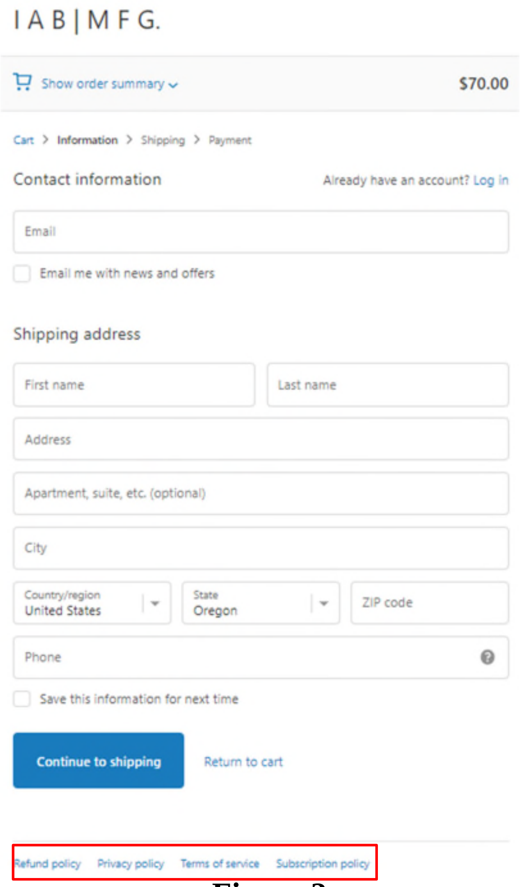
☑ Keep me up to date on news and exclusive offers

Country/Region United States

State Oregon

□ Save this information for next time

Figure 1



□ Email me with news and offers

Country/region United States

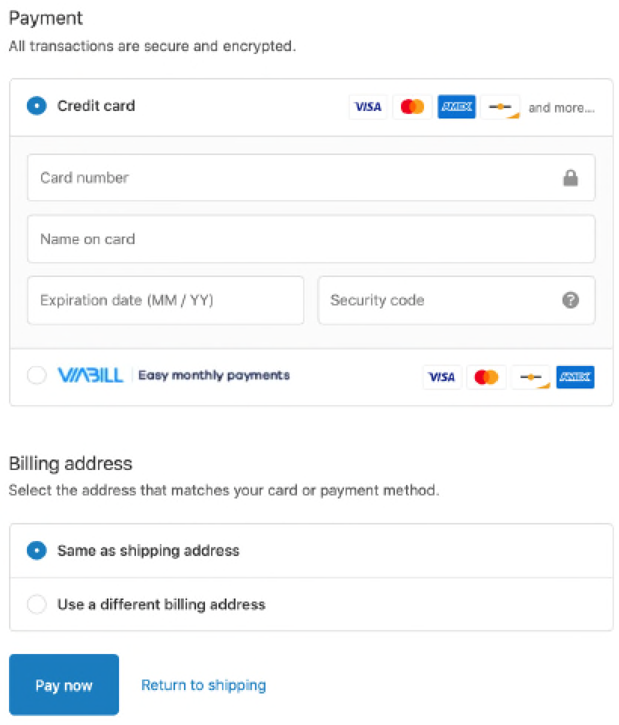
State Oregon

□ Save this information for next time

Figure 2

The image at FAC ¶ 21 is cropped so as to omit the portion of the screen below the "Continue to shipping" and "Return to cart" buttons, which presents shoppers with links to IABMFG's Refund Policy, Privacy Policy, and Terms of Service (**Fig. 2**). *See* Heath Decl., Ex. A (red box added).[2]

The same pages from which the FAC provides screenshots demonstrates that, in the course of checking out, consumers are provided with other links to IABMFG's Privacy Policy as well. For instance, the FAC alleges that after completing the above checkout screen (**Fig. 1**), Plaintiff was "required to provide his private information in order to complete the checkout process," FAC ¶ 52, on a screen like the one below (**Fig. 3**), FAC ¶ 24. As above, the full version of that screen (**Fig. 4**) includes a link to IABMFG's Privacy Policy. *See* Heath Decl., Ex. B (red box added). [3]



Payment

All transactions are secure and encrypted.

● Credit card VISA AMEX and more...

Card number

Name on card

Expiration date (MM / YY) Security code

○ VIABILL Easy monthly payments

Billing address

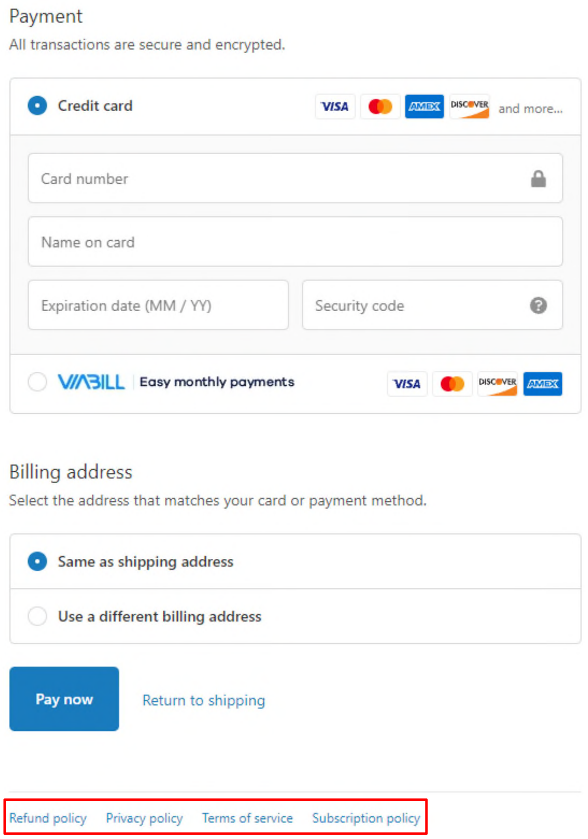
Select the address that matches your card or payment method.

● Same as shipping address

○ Use a different billing address

Pay now Return to shipping

Figure 3



Payment

All transactions are secure and encrypted.

● Credit card VISA AMEX DISCOVER and more...

Card number

Name on card

Expiration date (MM / YY) Security code

○ VIABILL Easy monthly payments

Billing address

Select the address that matches your card or payment method.

● Same as shipping address

○ Use a different billing address

Pay now Return to shipping

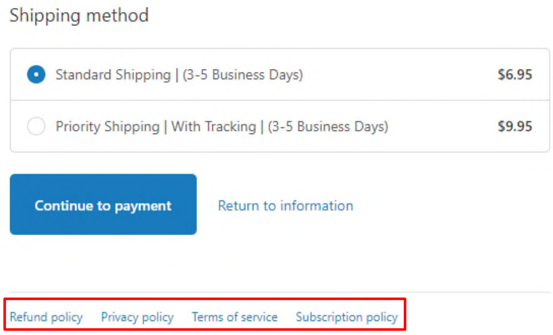
Refund policy Privacy policy Terms of service Subscription policy

Figure 4

[2] *Available at* https://www.iambecoming.com/4572025/checkouts/5a9f0424b4812fc7195441a3ff49d5b1.

[3] *Available at* https://www.iambecoming.com/4572025/checkouts/5a9f0424b4812fc7195441a3ff49d5b1?previous_step=shipping_method&step=payment_method.

When selecting the method for shipping his purchases, there too IABMFG's website presents a link to the Privacy Policy. (**Fig. 5**). *See* Heath Decl., Ex. C (red box added).[4]



Shipping method

● Standard Shipping | (3-5 Business Days) $6.95

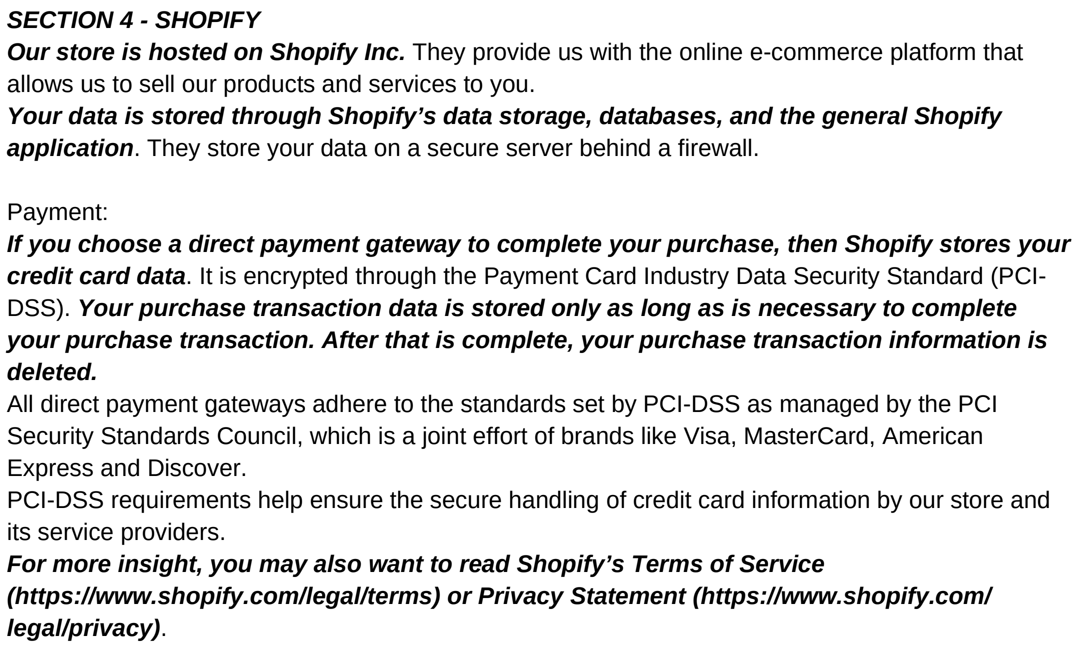
○ Priority Shipping | With Tracking | (3-5 Business Days) $9.95

Figure 5

In short, the website the FAC relies upon links to IABMFG's Privacy Policy for consumers at least three times (*see* **Figs. 2, 4, 5**) in the course of checkout, each situated in a distinct blue color, just under the buttons that Plaintiff was required to click on in order to advance with his purchase. Despite providing and relying on these screenshots and incorporating the webpages by reference, the FAC alleges "on information and belief" that "[a]t some point . . . after Plaintiff's transaction with IABMFG—the company modified its website" and that "Plaintiff never saw" the links to the Privacy Policy that clearly appear on the uncropped pages imaged in the FAC. FAC ¶ 54.

IABMFG's Privacy Policy linked on the pages the FAC provides in cropped form discloses (among other things) that IABMFG's online store is "hosted on Shopify Inc.," an "e-commerce platform that allows [merchants] to sell [their] products and services" online." Indeed, the Privacy Policy has an entire section dedicated to Shopify Inc. and its role, where it explains that a consumer's data is "stored through Shopify [Inc.]'s data storage, databases, and the general Shopify application," and that if a customer chooses certain payment methods, Shopify Inc. will "store[] [the consumer's] credit card data" for "only as long as is necessary to complete [the] purchase transaction," at which point the "purchase transaction information is deleted." IABMFG's Privacy Policy further directs readers to Shopify Inc.'s own Terms of Service and Privacy Statement in case they have additional questions about Shopify Inc.'s involvement, Heath Decl., Ex. D (emphasis added):

[4] *Available at* https://www.iambecoming.com/4572025/checkouts/5a9f0424b4812fc7195441a3ff49d5b1?previous_step=contact_information&step=shipping_method



SECTION 4 - SHOPIFY
Our store is hosted on Shopify Inc. They provide us with the online e-commerce platform that allows us to sell our products and services to you.
Your data is stored through Shopify's data storage, databases, and the general Shopify application. They store your data on a secure server behind a firewall.

Payment:
If you choose a direct payment gateway to complete your purchase, then Shopify stores your credit card data. It is encrypted through the Payment Card Industry Data Security Standard (PCI-DSS). ***Your purchase transaction data is stored only as long as is necessary to complete your purchase transaction. After that is complete, your purchase transaction information is deleted.***
All direct payment gateways adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, MasterCard, American Express and Discover.
PCI-DSS requirements help ensure the secure handling of credit card information by our store and its service providers.
For more insight, you may also want to read Shopify's Terms of Service (https://www.shopify.com/legal/terms) or Privacy Statement (https://www.shopify.com/legal/privacy).

Shopify Inc.'s own Privacy Statement, in turn, contains more detailed disclosures about what data it processes and how. It included a plainly worded explanation of how Shopify Inc. handled consumer data, covering topics including: "[w]hy we process your information," "[w]here we send your information," "[y]our rights over your information," and "[h]ow we use 'cookies' and other tracking technologies." Heath Decl., Ex. E. This last category includes a link to Shopify Inc.'s Cookie Policy, which provided more detail on every cookie that Shopify Inc. used, including name, function, and duration. Heath Decl., Ex. F.

The FAC nevertheless claims that Plaintiff "was not aware" that when he "submitted the form containing his private information to complete the checkout process, his private information was sent to Shopify[] [Inc.]'s computer network, where it was stored, analyzed, and processed." FAC ¶ 53. The FAC also asserts that Plaintiff "was not aware" that Shopify Inc. would "install[] a tracking cookie … on his smartphone." *Id.* The FAC alleges that "[h]ad [Plaintiff] known that Shopify [Inc.] would collect, store, and analyze his private information," he "would not have purchased products from IABMFG." FAC ¶ 57. In acknowledging the presence of disclosures of Shopify's involvement, the FAC claims that, nevertheless, "Plaintiff never saw nor agreed" to those "privacy disclosures on the IABMFG website." FAC ¶ 54.

On these bases, Plaintiff filed this lawsuit accusing Shopify Inc. of committing crimes and torts for processing his purchase information and utilizing routine cookies in exactly the manner those disclosures said it would.

III. LEGAL STANDARD

A motion to dismiss under Rule 8 is decided solely on the face of the complaint. A complaint survives such a motion only if it provides each "defendant[] fair notice of the claims against [it]." *Bravo v. Cnty. of San Diego*, 2014 WL 555195, at *2 (N.D. Cal. 2014). "[L]umping together multiple defendants in one broad allegation fails to satisfy [this] notice requirement." *Id.*

A motion to dismiss under Rule 12(b)(2) is not limited to the pleadings and "may consider extrinsic evidence … including affidavits submitted by the parties." *Stewart v. Screen Gems-EMI Music, Inc.*, 81 F. Supp. 3d 938, 951 (N.D. Cal. 2015). The plaintiff bears the burden of establishing personal jurisdiction. *Pebble Beach Co. v. Caddy*, 453 F.3d 1151, 1154 (9th Cir. 2006).

A motion to dismiss under Rule 12(b)(6) is resolved solely on the face of the complaint. To survive a motion under Rule 12(b)(6), "a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "[L]abels and conclusions, and a formulaic recitation of the elements" of claims will not suffice. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

IV. LEGAL ARGUMENT

A. The FAC Fails Under Rule 8 Because It Fails to Distinguish Among Defendants.

As explained in detail in Shopify USA's MTD Brief, the FAC must be dismissed because, by combining Shopify Inc. and Shopify USA into a fictitious single entity that it defines as "Shopify," the FAC fails to provide either Shopify Inc. or Shopify USA with sufficient notice of the claims against it, as required by Rule 8. *See* Shopify USA MTD Br. § IV.A.

B. This Court Lacks Jurisdiction Over Shopify Inc.

1. *This Court lacks general jurisdiction over Shopify Inc.*

The "paradigm forums" for general jurisdiction over a corporation are "the corporation's place of incorporation and its principal place of business." *BNSF Ry. Co. v. Tyrrell*, 137 S. Ct. 1549, 1558 (2017). General jurisdiction outside of those forums is available "[o]nly in an exceptional case," *Martinez v. Aero Caribbean*, 764 F.3d 1062, 1070 (9th Cir. 2014), where the defendant's contacts are so "continuous and systematic" as to "'approximate physical presence' in the forum state," *Pestmaster Franchise Network, Inc. v. Mata*, 2017 WL 1956927, at *2 (N.D. Cal. 2017). Here, as Judge Chen recently recognized, there is no basis for asserting general jurisdiction against Shopify Inc. under either theory. *See Baton v. Ledger*, 2021 WL 5226315, at *3 (N.D. Cal. 2021) (dismissing Shopify Inc. for lack of jurisdiction).

As in *Baton*, the FAC here admits that California is not one of the "paradigm forums" where general jurisdiction over Shopify Inc. is proper. *See id.* at *3. It concedes that Shopify Inc. is incorporated not in California, but rather in "Canad[a]," and that its principal place of business is in "Ottawa, Canada." FAC ¶ 9. Thus the "only remaining theory for the Court to assert general jurisdiction is that this is 'an exceptional case'" where Shopify Inc.'s "contacts are so continuous and systematic as to approximate physical presence in California." *Baton*, 2021 WL 5226315 at *4. But, as Judge Chen recently noted, the plaintiffs in *Baton* did not even attempt to argue that such a finding could be made as to Shopify Inc. *Id.* at *3. And for good reason. Shopify Inc. "has no offices or staff in California, is not registered to do business in the state, has no registered agent for service of process, and pays no state [income] taxes." *Mavrix Photo, Inc. v. Brand Techs., Inc.*, 647 F.3d 1218, 1225 (9th Cir. 2011) (finding no general jurisdiction for that reason); *see* Heath Decl., Ex. G ¶¶ 5-6.[5] There is thus no basis for asserting general jurisdiction over Shopify Inc.

2. *This Court lacks specific jurisdiction over Shopify Inc.*

Specific jurisdiction exists only when (1) the defendant "purposefully direct[s] his activities" toward the state or its residents; and (2) the claim before the court "arises out of or relates to the defendant's forum-related activities." *Caces-Tiamson v. Equifax*, 2020 WL 1322889, at *3 (N.D. Cal. 2020). Here, the FAC fails to allege any facts to establish those prerequisites as to Shopify Inc.

To satisfy the requirements of specific jurisdiction, the FAC must plead facts showing an

[5] Exhibits G and H to the Heath Declaration are sworn declarations by employees of Shopify Inc. and Shopify USA, which were recently submitted in *Baton v. Ledger*, No. 21-cv-2470, ECF. No. 56-1 (N.D. Cal.) (executed and filed July 26, 2021). The facts in those declarations cited here remain accurate.

(1) "intentional act" on the part of Shopify Inc. "(2) expressly aimed at the forum state, (3) causing harm that [Shopify Inc.] knows is likely to be suffered in the forum state." *Dole Food Co. v. Watts*, 303 F.3d 1104, 1111 (9th Cir. 2002). But the FAC makes no allegations meeting the test. Rather, all it alleges is that Shopify Inc. provides its software to "millions" of merchants around the world, operating "millions of websites," one of whom happens to be IABMFG (who in turn sold goods to Plaintiff in California), and that IABMFG obtained and "integrate[d]" that software into its own universally accessible website. *See, e.g.*, FAC ¶¶ 1-2, 6-7. That is plainly insufficient. As Judge Chen explained, Shopify Inc. (or, indeed, any company) does not purposefully direct acts into California "based on the mere fact that [it] provides services to customers [merchants] nationwide," even if some of those customers happen to be located in California. *Baton*, 2021 WL 5226315, at *6. Because the FAC alleges no facts demonstrating that Shopify Inc. directed acts towards California in any way distinct from the rest of the world, it has failed to carry the burden of pleading facts sufficient to establish specific jurisdiction over Shopify Inc.

C. The FAC Fails to State a Claim Against Shopify Inc.

The FAC also must be dismissed in its entirety as to Shopify Inc. under Rule 12(b)(6) because the FAC itself (along with IABMFG webpages incorporated by reference therein, *see supra* § II) makes clear that Plaintiff consented to any data collection, which defeats each of Plaintiff's claims. Additionally, independent of the issue of consent, each of the FAC's claims—under (1) Section 631; (2) Section 635; (3) the California constitution or common law; (4) Section 502; (5) the Unfair Competition Law; and (6) the right of publicity—must fail.

1. *The FAC fails to state any claim because it pleads facts showing that Plaintiff consented to any data collection.*

It is well-established that "[c]onsideration of consent is appropriate on a motion to dismiss where lack of consent is an element of the claim." *Silver v. Stripe Inc.*, 2021 WL 3191752, at *2 (N.D. Cal. 2021). That is true of every one of Plaintiff's claims here:

Section 631 applies, by its terms, only where a defendant acts "without … ***consent***" or in an "unauthorized" manner. Cal. Penal Code § 631(a) (emphasis added); *see also Stripe*, 2021 WL 3191752, at *3 (relying on plaintiff's consent to dismiss Section 631 claim under Rule 12(b)(6)).

A **Section 635** claim likewise "also depends on ***consent***" (or lack thereof) to be viable, because such a cause of action requires "injur[y]." *Stripe*, 2021 WL 3191752, at *3 (relying on plaintiff's consent to dismiss Section 635 claim under Rule 12(b)(6)) (emphasis added); *see also* Cal. Penal Code § 637.2(a) (providing a cause of action for a violation of Section 635 only to a "person who has been injured").

Invasion of Privacy under the California Constitution occurs only where a plaintiff has "conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have manifested by his or her conduct a voluntary ***consent*** to the invasive actions of the defendant." *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 955-956 (N.D. Cal. 2017) (relying on plaintiff's consent to dismiss invasion of privacy claim under Rule 12(b)(6)) (emphasis added), *aff'd*, 745 F. App'x 8 (9th Cir. 2018).

Intrusion Upon Seclusion likewise occurs only if the plaintiff establishes that he had a reasonable expectation of privacy, which does not exist where a plaintiff gives consent to the defendant's acts. *See Smith*, 262 F. Supp. 3d at 955-956 (relying on plaintiff's consent to dismiss intrusion upon seclusion claim under Rule 12(b)(6)); *see also Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016) ("Effective ***consent*** negates an intrusion upon seclusion claim." (emphasis added)).

Section 502 applies only to a person who accesses a computer and performs acts "without permission"—an element that is not met if plaintiff gives consent to the access or acts. *Brown v. Google LLC*, 2021 WL 949372, at *7 (considering whether plaintiff consented to evaluate Rule 12(b)(6) motion to dismiss Section 502 claim).

The FAC's **UCL** claim "is predicated on [Shopify Inc.]'s representations and Plaintiff's other claims," so consent is a proper basis for dismissal for this claim too. *Calhoun v. Google LLC*, 2021 WL 1056532, at *7, n.3. (N.D. Cal. 2021) (considering whether plaintiff consented to evaluate Rule 12(b)(6) motion to dismiss UCL claim).

And a **right of publicity** claim, whether under the common law or statute, requires as an element a "lack of consent," *Gionfriddo v. Major League Baseball*, 94 Cal. App. 4th 400, 409 (2001); *see also* Cal. Civ. Code § 3344(a) (creating a cause of action where defendant acts "without such person's prior consent").

A user consents to activities disclosed in a website's privacy notice when he uses the website with at least "constructive knowledge of [the] website's terms and conditions." *Dohrmann v. Intuit, Inc.*, 823 F. App'x 482, 483-84 (9th Cir. 2020) (quoting *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1176 (9th Cir. 2014)). Constructive knowledge exists where the website "put[s] 'a reasonably prudent user on inquiry notice'" of the terms. *Stripe*, 2021 WL 3191752, at *3. That condition is met where a user is "provided with an opportunity to review the terms of service" through a "hyperlink." *Id.*

That is precisely what happened here. As the webpages incorporated by reference in the FAC demonstrate, IABMFG's Privacy Policy was prominently displayed throughout Plaintiff's entire IABMFG purchase experience, and it explicitly disclosed Shopify Inc.'s role in collecting data. *See supra* § II. In fact, an entire section of the IABMFG Privacy Policy was dedicated solely to Shopify Inc., and specifically disclosed not only that IABMFG's store was "hosted on Shopify Inc." and that "your data is stored through Shopify [Inc.]'s data storage, databases and the general Shopify application," but also that "[i]f you choose a direct payment gateway to complete your purchase, then Shopify [Inc.] stores your credit card data" for "as long as is necessary to complete your purchase transaction" and then deletes "your purchase transaction information" as soon as the transaction "is complete." Heath Decl., Ex. E. Additionally, IABMFG's Privacy Policy went further, advising that users "may also want to read Shopify [Inc.]'s Terms of Service and Privacy Statement" and providing links to each. *Id.* Each of Shopify Inc.'s Terms of Service and Privacy Statement in turn provided a detailed description of what Shopify Inc. did with a consumer's purchase data, what cookies Shopify Inc. installed when a user visits a merchant's website, what those cookies did, and how long they persisted. *See supra* § II.

As noted above, the FAC attempts to plead around these disclosures by alleging that Plaintiff, based "on information and belief," "never saw nor agreed to any privacy disclosures on the IABMFG website," because IABMFG "modified its website" to include these links to the Privacy Policy only "after Plaintiff's transactions with IABMFG." *Compare* FAC ¶ 54, *with* Compl. ¶ 52 (making no such allegation). That allegation should be disregarded in full. First, this new "information and belief" allegation is "conclusory in nature" unsupported by any alleged fact, and "[o]n that basis alone" must be "disregard[ed] under *Iqbal* and *Twombly*." *Sims v. Opportunity Fin., LLC*, 2021 WL 1391565, at *8 (N.D. Cal. 2021) (Hamilton, J.). Second, the allegation is negated by the FAC's incorporation of IABMFG's website as the basis for Plaintiff's claims. *See supra* § II; *see also, e.g.*, FAC ¶¶ 21-27, 50-54 (quoting, describing, and including images of IABMFG's current website). When "the FAC, when read as a whole, does not support plaintiff's information and belief allegation," that allegation may be disregarded. *Sims*, 2021 WL 1391565, at *8; *see also Soo Park v. Thompson*, 851 F.3d 910, 928 (9th Cir. 2017) (*Twombly* allows information and belief allegations "where the belief is based on factual information that makes the inference … plausible").

The IABMFG website makes clear that Plaintiff was at a minimum on inquiry notice of IABMFG's Privacy Policy. There can be no doubt that IABMFG's website "provided [users] with an opportunity to review" the Privacy Policy through a "hyperlink." *Stripe*, 2021 WL 3191752, at *3. Indeed, it does so three times—presenting prominent hyperlinks to IABMFG's Privacy Policy on the checkout, payment, and shipping pages. *See supra* § II. Each time, that information appears immediately under the buttons that Plaintiff was required to press to proceed or turn back. *See id.* As a matter of law, that is sufficient to create the notice required to make the terms of IABMFG's Privacy Policy binding.[6] *See Stripe*, 2021 WL 3191752, at *3. IABMFG's website presents consumers with at least three opportunities to learn of Shopify Inc.'s involvement in any transaction. Whether Plaintiff chose to avail himself of any does render Shopify Inc.'s routine processing of his transaction criminal.

Stripe is instructive. The *Stripe* Court's reasons for finding the privacy policy there "conspicuous and obvious" map onto this case directly:

> First, the hyperlink to [IABMFG's] privacy policy is displayed in a bright [blue]

[6] This should not be controversial. An IABMFG consumer could not avoid IABMFG terms—say its 60-day refund policy, *see* Heath Decl., Ex. J—by claiming it was not binding because the consumer did not choose to view it. By proceeding to complete a purchase on IABMFG's website, which prominently links at least thrice to IABMFG's refund policy, the consumer is bound by those terms. The link to IABMFG's Privacy Policy is no different. It was presented in exactly the same way—and, in fact, immediately next to—the link to IABMFG's Refund Statement. *See supra* § II.

> font against a white background, which stands out from most of the surrounding text. Further, the hyperlink to the privacy policy is located close to the "place order" button, thus it is hard for a user placing an order to miss it. The bold font alerting consumers to the amount of the charge … placed on their card calls additional attention to the area where [IABMFG's] privacy policy is located. There is nothing about the text that makes it inconspicuous or nonobvious.

2021 WL 3191752, at *3. The same result should obtain here.

2. *The FAC fails to state an eavesdropping claim under Penal Code Section 631(a).*

Separate and apart from the categorical legal bar that Plaintiff's consent poses to his suit, the FAC fails to state an eavesdropping claim under Section 631(a) for processing Plaintiff's transaction. That provision makes it unlawful to (1) "intentionally tap[], or make[] any unauthorized connection … with any telegraph or telephone wire, line, cable, or instrument," or (2) "willfully and without the consent of all parties to the communication … read[], or attempt[] to read, or to learn the contents or meaning of any message … while the same is in transit." Cal. Penal Code § 631(a). As discussed below, the FAC fatally fails to allege that *any* third-party disclosure occurred at all. It also fails to allege tapping of a telephone line required under clause 1, or unauthorized disclosure of contents required under clause 2, thus failing to state any claim under Section 631(a).[7]

a. The FAC fails to state a claim under either clause of Section 631(a), because it fails to plead facts showing that Shopify Inc. was a third party to Plaintiff's communications.

To state a claim against Shopify Inc. under any clause of Section 631, the FAC must allege facts showing that Shopify Inc. was a third party to Plaintiff's communications. That is because Section 631 "'appl[ies] only to eavesdropping by a third party.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 607 (9th Cir. 2020) (quoting *Warden v. Kahn*, 99 Cal. App. 3d 805, 811 (1979). It does not cover "a participant"—even one who "record[s]" the communication. *Id.*

Here, that rule means—undisputedly—that IABMFG cannot be liable under Section 631(a),

[7] It is unclear whether Plaintiff also means to invoke Section 631's third clause, which makes it a crime to "use[], or attempt[] to use, … or to communicate … any information so obtained." But that clause applies only where the information at issue "was obtained through a violation of the first or second clauses." *In re Google Assistant Privacy Litig.*, 2020 WL 2219022, at *16. Because Plaintiff cannot show a violation of either of those clauses, he "also ha[s] failed to plead a violation of the third clause." *Id.* The same is true of Section 631's fourth clause as well, which criminalizes aiding and abetting violations of the first two clauses.

as the FAC concedes that IABMFG was the intended recipient of Plaintiff's information. FAC ¶ 52. But that same rule means that Shopify Inc. cannot be liable either, because Shopify Inc. received Plaintiff's information not as an independent "third party" interloping on Plaintiff's communications with IABMFG, but rather as "an extension of" IABMFG itself. *Graham v. Noom, Inc.*, 2021 WL 1312765, at *5 (N.D. Cal. 2021). Specifically, Shopify Inc. is "a vendor that provides a software service" to IABMFG—namely, tools that "capture its clients' data, hosts it on [Shopify Inc.]'s servers, and allows the clients to analyze their data." *Id.* Said otherwise, Shopify Inc. "provide[d] a tool" that IABMFG chose to employ "to record and analyze its own data in aid of [its own] business." *Id.* This is not a case where a third-party surreptitiously redirected communication away from its intended recipient, but one where the intended recipient itself contracted with another to act in its stead—no different than when a company employs an outside call center to field customer inquiries on its behalf. *See Allen v. Quicken Loans Inc.*, 2018 WL 5874088, at *4 (D.N.J. 2018) (third-party Javascript code hosted on a website is not an unlawful wiretap under analogous provision of federal Wiretap Act). Because Shopify Inc. was not a third-party to any of Plaintiff's communications, it cannot be deemed to have violated Section 631(a).

b. <u>The FAC fails to allege a violation of Section 631(a)'s first clause, because it fails to allege a wiretap of a telephone line.</u>

In any event, the FAC separately fails to state a claim under the first clause of Section 631(a), which makes a defendant liable only if it taps a "telegraph or telephone wire, line, cable, or instrument." Cal. Penal Code § 631(a). That clause requires a plaintiff to allege not only that a defendant tapped a "wire, line, cable, or instrument" but, also that whichever of those was involved carried "telegraph or telephone" signals. *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 825-26 (N.D. Cal. 2020) (holding that complaint failed to state a claim under Section 631(a) because it did not suggest "that Google Assistant operates using telegraph or telephone wires").

Here, the FAC alleges no facts suggesting that any services Shopify Inc. provides to IABMFG operate via (much less "tap") "telegraph or telephone" lines. In fact, the FAC says otherwise, alleging that Shopify Inc.'s technology "tapped, electrically or otherwise, the lines and/or instruments of *internet communication*." FAC ¶ 77; *see also id.* ¶ 50. "[I]nternet communication" however, does not take place (at least, nowadays) over "telephone" or "telegraph" lines. *See Verizon v. FCC*, 740 F.3d 623, 629 (D.C. Cir. 2014) (explaining that while in the "early days" users "connected to the Internet through dial-up connections over local telephone lines," access has, at least since 2014, been "furnished through" other technologies like "broadband"). With that allegation, the FAC has effectively "ple[d] [itself] out of court by alleging facts which show that [Plaintiff] has no claim." *See Sprewell v. Golden State Warriors*, 266 F.3d 979, 988-89 (9th Cir. 2001) (affirming dismissal because plaintiff's complaint included "unnecessary details contrary to his claims").

The FAC insists that "Section 631(a) is not limited to phone lines, but also applies to 'new technologies,' such as computers, the Internet, and email." FAC ¶ 72. But that is because *the second clause* applies (per its text) to "communications passing over '*any* wire, line, or cable.'" *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 826 (citation omitted); *see also Matera v. Google, Inc.*, 2016 WL 8200619, at *18 (N.D. Cal. 2016). The *first clause* of that provision (the subject of this discussion) is "limited to communications passing over 'telegraph or telephone' wires, lines, or cables." *Matera*, 2016 WL 8200619, at *18; *accord In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 826. Courts have thus held that it is inapplicable to technologies operating over the internet—including on smartphones. *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 826; *see also* FAC ¶ 50 (alleging that Plaintiff "used his iPhone's Safari browser" to visit IABMFG's website). Accordingly, the FAC fails to state a claim under the first clause of Section 631(a) because it has not alleged that Shopify Inc. tapped "telegraph or telephone" wires.

c. <u>The FAC fails to allege a violation of Section 631(a)'s second clause because it fails to plead facts showing that Shopify Inc. read the "contents" of any message.</u>

The FAC separately fails to state a claim under Section 631(a)'s second clause, which prohibits only the "unauthorized access of the 'contents' of any communication." *See Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020). The "contents" of a communication under Section 631 has the same meaning as under the federal Wiretap Act—i.e., "the intended message conveyed by the communication." *See In re Zynga Privacy Litig.*, 750 F. 3d 1098, 1106 (9th Cir. 2014). That means to state a claim under Section 631(a)'s second clause, two things must be true:

(1) a plaintiff must have intended to convey a substantive message, and (2) the defendant must have accessed (or attempted to access) that substance, and not mere "record information," like name and address, that merely facilitates a communication or transaction. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012) (holding that "data" that is "generated" without the communicative "intent of the user" cannot "constitute 'content' susceptible to interception"); *see also Svenson v. Google Inc.*, 65 F. Supp. 3d 717, 729 (N.D. Cal. 2014) (explaining that "names, mailing addresses, phone numbers, billing information, and date of account creation," have been characterized as "record or other information" and not "contents" of a communication (citing *Chevron Corp. v. Donziger*, 2013 WL 4536808, at *6 (N.D. Cal. 2013)).

Here, the FAC asserts that "in order to complete the checkout process," Plaintiff provided "his full name, delivery address, billing address, phone number, and credit card number, expiration date, and CVV code," which Shopify Inc. collected. FAC ¶ 52. But, for two reasons, that fails to satisfy the "content" requirement necessary to state a claim. *First*, Plaintiff's provision of information necessary to complete a commercial checkout transaction is not the same as composing a message with substantive, communicative intent; that is, there was no "intended message conveyed" by Plaintiff here at all. *See Zynga*, 750 F.3d at 1106. *Second*, every type of information that the FAC identifies falls into the classes of data held to be mere record information—i.e., the kind of information that merely facilitates a communication or transaction—not message "content." *Compare* FAC ¶ 52 ("name, delivery address, billing address, phone number, and credit card number, expiration date, and CVV code"), *with, e.g.*, *Svenson*, 65 F. Supp. 3d at 729 ("names, mailing addresses, phone numbers, billing information" are not content).[8] Accordingly, the FAC fails to state a claim under Section 631(a)'s second clause.

3. *The FAC fails to state a claim under Penal Code Section 635.*

Section 635 makes it a crime to "manufacture[], assemble[], sell[], offer[] for sale, advertise[] for sale, possess[], transport[], import[], or furnish[] to another any device which is

[8] *See also Zynga*, 750 F. 3d at 1106 ("contents" does not include "information regarding the characteristics of the message that is generated in the course of the communication" like "the name, address, and subscriber number or identity of a subscriber or customer"); *Brodsky*, 445 F. Supp. 3d at 127 ("user names, passwords, and geographic location information" are not "content[]").

primarily or exclusively designed or intended for eavesdropping." Cal. Penal Code § 635(a). The FAC asserts that Shopify Inc. violated that provision by possessing "software code modules" designed to collect and process his shipping, billing, and payment information as required to facilitate his purchase from IABMFG. FAC ¶¶ 84-85. That theory fails for two reasons.

a. The Section 635 claim fails because code is not a "device" within the meaning of the California Invasion of Privacy Act.

The FAC's Section 635 claim is premised on the assumption that Shopify Inc.'s "software code modules" constitutes a "device." FAC ¶¶ 84-85.[9] But every usual indicator of statutory meaning—text, context, history, and the rule of lenity—make clear that Section 635 uses the term "device" in a way that connotes a physical object, and hence excludes the computer code alleged by the FAC.

Text. By using the term "device" without specifically defining it, Section 635 directs courts to apply its ordinary meaning. *DeGeorge v. U.S. Dist. Court*, 219 F.3d 930, 936 (9th Cir. 2000); *accord, e.g.*, *De Vries v. Regents of Univ. of Cal.*, 6 Cal. App. 5th 574, 591 (2016). And a "device," in common parlance, is "a piece of equipment or a mechanism designed to serve a special purpose or perform a special function." Webster's Third New International Dictionary of the English Language Unabridged 618 (2002); *see also Consolidation Coal Co. v. Fed. Mine Safety & Health Review Comm'n*, 136 F.3d 819, 822 (D.C. Cir. 1998). That definition—and particularly, its references to "equipment" or "a mechanism"—connotes a physical object.

Context. The list of acts that Section 635 forbids one to do with a "device" confirms that the provision contemplates only physical objects. Specifically, Section 635 makes it unlawful to (among other things) "manufacture[]," "assemble[]," "transport[]," or "import[]," a device. While one could readily do any of those things to physical objects, it would be odd and inappropriate word choice to apply any of those verbs to intangible software code.

[9] That the FAC alleges that "code" is a "device," FAC ¶ 84, is irrelevant. The "proper definition" of a statutory term is a "[p]urely legal question[.]" *Freeman v. Gonzales*, 444 F.3d 1031, 1037 (9th Cir. 2006). And courts, even at the motion-to-dismiss stage, "are not bound to accept … a legal conclusion" as true. *Iqbal*, 556 U.S. at 678-79; *see also, e.g.*, *Schlegel v. Wells Fargo Bank, NA*, 720 F.3d 1204, 1208-09 (9th Cir. 2013) (affirming dismissal on grounds that complaint's allegation that "Wells Fargo is in the business of collecting debts" was insufficient to show that it met the statutory definition of a "debt collector").

History. Section 635 provision was enacted in 1967, well before anyone could have imagined that computer code could play any role in surveillance or eavesdropping. *See History of Digital Recording*, https://recording-history.org/history-of-digital-recording (explaining that digital audio recording was not even commercially available until 1977, and even then it was stored on physical tapes, not computer-accessible media). There is no indication that, as enacted, Section 635 was intended to include future computer code. Nor did the Legislature signal an intent to change that when it most recently updated the provision to account for "new technological devices" in 1990. 1990 Cal. Legis. Serv. 696, § 2(d) (West). To the contrary, the Legislature made clear that the new devices it was concerned about were physical objects that had the capability to intercept transmissions from "cordless telephone unit[s]." *Id.* § 2(b). Indeed, the legislature specifically disclaimed an intent for its amendment to apply to anything beyond the "interception or reception of cordless telephone radio frequencies." *Id.* § 2(f). And as explained above (at § IV.C.2.b), the code here has nothing to do with telephone transmissions.

Lenity. Because Section 635 is a criminal statute, the rule of lenity requires that any ambiguity about whether the term "device" includes computer code must be resolved in favor of a narrower reading. *People v. Robles*, 5 P.3d 176, 182 (Cal. 2000); *see also Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) (lenity applies to noncriminal applications of a criminal statute.).

Accordingly, computer code does not constitute a "device" within the meaning of Section 635. The FAC, therefore, fails to state a claim under that statute as a matter of law.

b. The Section 635 claim fails because the FAC fails to allege facts showing that Shopify Inc.'s code was "primarily or exclusively designed" for eavesdropping.

The FAC's Section 635 claim also fails for the independent reason that Shopify Inc.'s code was not "primarily or exclusively designed or intended for eavesdropping upon the communication of another." Cal. Penal Code § 635. Under Section 635's plain and ordinary meaning, it is not sufficient that a device be merely capable of eavesdropping. Rather, the "device" must be "exclusively" or "primarily" geared toward eavesdropping. This construction is sensible. Otherwise a broad swath of devices—e.g., microphones, tape recorders, and cellphones—that could be used to eavesdrop, even though eavesdropping is not their primary or exclusive design, would be criminalized, and criminal liability imposed on all who "manufacture[], assemble[], sell[], offer[] for sale, advertise[] for sale, possess[], transport[], import[], or furnish[]" such products. *See, e.g.*, *United States v. Schweihs*, 569 F.2d 965, 968 (5th Cir. 1978) (observing that Congress, when it passed a federal analogue of CIPA, did not wish to attach criminal liability to "legitimate electronic device[s]" merely because they *could be* used for eavesdropping, but only to devices specifically designed for that end like "microphones disguised as wristwatches and fountain pens.").

The FAC's theory seems to be that any time a consumer's information is transmitted to a payment processor to complete an online purchase, a criminal violation of Section 635 has been committed. That position is astounding in its breadth: The factual core of the FAC's objection—that "card information is captured" "[d]uring the transaction" "and transmitted to a payment [processor]"—is standard, not just in online purchases, but in physical ones too. *CFPB v. Universal Debt & Payment Sols., LLC*, 2015 WL 11439178, at *1 (N.D. Ga. 2015); *see also Cohen v. Casper Sleep Inc.*, 2018 WL 3392877, at *4 (S.D.N.Y. 2018) (explaining that many websites install code to collect data, not with the "primary motivation" of spying on their users, but to help with legitimate purposes such as marketing); FAC ¶ 35 ("[O]ver one million websites and other merchants use Shopify [Inc.] to sell their products."). Indeed, it is what "enable[s] merchants to accept check, card, and electronic payments" at all. *Universal Debt*, 2015 WL 11439178, at *1. Accordingly, to the extent Section 635 applies to computer code at all (*see supra* § IV.C.3.a), it must be enforced according to its text and only applied to the code that is "exclusively" or "primarily" designed for an illicit purpose—lest it criminalize the billions of legitimate credit card transactions that form the backbone of the modern economy.

Here, the FAC alleges that because Shopify Inc.'s code is "designed to intercept, collect, transmit, receive, and track communications that [Plaintiff] reasonably (but erroneously) believed would be sent directly and exclusively to [IABMFG]," it was "'primarily or exclusively designed or intended for eavesdropping." FAC ¶ 85. That allegation is belied by the other allegations regarding Shopify Inc.'s actual role in the online purchasing ecosystem. FAC ¶ 17 ("Shopify is an e-commerce platform that enables merchants to sell products online."). And, even then, that allegation is nothing more than a "legal conclusion couched as a factual allegation," which need not be credited. *Iqbal*, 556 U.S. at 678. The allegedly offending code is no more "designed" to eavesdrop than every credit card processing terminal in physical stores everywhere.

When it comes to actual facts, the FAC's allegations go solely to what Shopify Inc.'s code does (i.e., capture payment data for the purpose of facilitating transactions); nothing in those allegations suggest the purpose to eavesdrop. *See, e.g.*, FAC ¶¶ 18, 53. In fact, to the extent the FAC's allegations shed light on the purpose behind Shopify Inc.'s code, they *negate* any suggestion that the code was "primarily or exclusively" intended for eavesdropping. The FAC admits, for instance, that Shopify Inc.'s "default template for merchant websites" includes a "'powered with Shopify' link leading to Shopify [Inc.]'s homepage." FAC ¶ 46. The FAC offers no theory for how defaulting merchants into a website design that discloses Shopify Inc.'s involvement evinces that the *primary* or *exclusive* intent of Shopify Inc.'s code was to hide Shopify Inc.'s involvement.

The FAC's allegations are at best "merely consistent with" a theory that leads to liability. But to survive dismissal under Rule 12(b)(6), it must provide "[s]omething more," "such as facts tending to exclude the possibility that the [innocent] explanation is true." *See In re Century Aluminum Co. Sec., Litig.*, 729 F.3d 1104, 1108 (9th Cir. 2013). Because the FAC pleads no facts showing that Shopify Inc.'s code was "primarily or exclusively" intended for eavesdropping, instead of facilitating legitimate purchase transactions, the Section 635 claim must be dismissed.

4. *The FAC fails to state a claim for invasion of privacy and intrusion upon seclusion because it does not allege facts showing that Shopify Inc. committed an "egregious" or "highly offensive" privacy intrusion.*

To allege a violation of California's constitutional right to privacy, the FAC must allege, among other things, "conduct by the defendant that amounts to a serious invasion of [a] protected privacy interest." *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 829 (N.D. Cal. 2020). To state a claim for intrusion upon seclusion, "a plaintiff must allege intrusion into a private place, conversation or matter in a manner highly offensive to a reasonable person." *Id.* at 830 (numbering omitted). Because the standards for these two causes of action "are closely related," courts "treat[] them together." *Id.* at 829; *see also Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009).

To show the requisite "serious invasion" or "highly offensive" intrusion, the FAC must allege facts showing an "egregious breach of the social norms"—a "high bar" that is not satisfied by "[e]ven disclosure of personal information, including social security numbers." *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012). "[C]ollection—and even disclosure to certain third parties—of" more anodyne "personal information" falls well below the requisite threshold. *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 829-30; *see also In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (no intrusion claim based on collection and disclosure of users' data, including browsing histories); *Low*, 900 F. Supp. 2d at 1025 (no "highly offensive" invasion of privacy by disclosing users' browsing histories to third parties). Where a party does nothing more than engage in "routine commercial behavior," it does not commit a violation of California's constitution or common-law privacy protections. *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d at 830. That is true even where the "routine commercial behavior" involves "obtaining [a] plaintiff's address without his knowledge or permission, and using it to mail him coupons and other advertisements." *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011) (finding such conduct not an "egregious breach of social norms").

Here, the FAC fails to establish that Shopify Inc.'s conduct was even as egregious as conduct held insufficient elsewhere. First, as the IABMFG webpages incorporated by reference into the FAC reveal, Shopify Inc.'s activity was fully disclosed. *See supra* § IV.C.1. Second, even if that were not true, what the FAC accuses Shopify Inc. of here—collecting purchase information to facilitate commercial transactions and installing routine cookies to improve website performance—happens on practically every website that offers goods or services in exchange for payments. *See In re Pharmatrak, Inc.*, 329 F.3d 9, 14 (1st Cir. 2003) ("Cookies often store user preferences, login and registration information, or information related to an online 'shopping cart.'"). Because the FAC has alleged no facts that mark Shopify Inc.'s conduct as being particularly egregious, rather than a commonplace part of the modern internet economy, his constitutional and common law privacy claims fail.

5. *The FAC fails to state a Penal Code Section 502 claim, because it fails to allege facts showing that Shopify Inc. accessed Plaintiff's iPhone "without permission."*

Section 502 criminalizes various acts that a person commits after having accessed data on a computer "without permission." Cal. Penal Code § 502; *see In re Google Android Consumer*

Priv. Litig., 2013 WL 1283236, at *11 (N.D. Cal. 2013). Courts in this District have been clear that the phrase "without permission" requires far more than merely acting without affirmatively obtaining a person's consent. (Although, as explained above, Plaintiff did give his consent. *See supra* § IV.C.1.) Specifically, a person "may only be subjected to liability for acting 'without permission' under Section 502 if they "access[ ] or us[e] a computer, computer network, or website in a manner that overcomes technical or code-based barriers." *In re iPhone Application Litig.*, 2011 WL 4403963, at *12 (N.D. Cal. 2011); *see also, e.g.*, *In re Facebook Priv. Litig.*, 791 F. Supp. 2d 705, 716 (N.D. Cal. 2011) ("It is thus impossible, on Plaintiffs' own allegations, for Defendant to be liable under the subsections of Section 502 which require a defendant to act "without permission," as there were clearly no technical barriers blocking Defendant from accessing its own website."), *aff'd*, 572 F. App'x 494 (9th Cir. 2014).

Here, the FAC includes no allegations that any of Shopify Inc.'s alleged activities overcame any technical or code-based barriers. Indeed, the FAC does not identify any technical or code-based barrier that Plaintiff deployed at all—much less one that Shopify Inc.'s overcame. Rather, the FAC's sole theory is that Shopify Inc. "surreptitiously and intentionally install[ed] software code and cookies" onto "Plaintiff's iPhone," and thus did so even though Plaintiff "never consented" to those acts. FAC ¶¶ 116-17. Of course, as explained above, that is simply incorrect. *See supra* § IV.C.1. But even if it were true, it would still be insufficient to state a claim under Section 502: As explained just above, Section 502 is violated only when a defendant overcomes a technical or code-based barrier; merely "caus[ing] 'nonconsensual transmissions' of [Plaintiff's] personal information as a consequence of Defendant's" operation of "its own website" is not enough. *See In re Facebook Priv. Litig.*, 791 F. Supp. 2d at 716.

In fact, the FAC's allegations make clear it asks the Court to bless an overly broad reading of Section 502. The "software code and cookies" that form the basis of this claim appear to refer to the "Shopify[Inc.]-produced javascript code" that makes IAMBFG's website run, FAC ¶ 26, and the routine cookies that identify, e.g., the user's device or country, FAC ¶¶ 32-33. If a violation of Section 502 occurs any time a person voluntarily visits a website, and that website installs javascript code or cookies in his browser, without him being specifically aware of each line of code, each and every cookie, and the identity of the person or vendor responsible for producing that code, then this provision would criminalize essentially *every* website on the internet. The Northern District of California's homepage, for instance, installs javascript code without affirmatively telling the user that it is doing so. *See* https://cand.uscourts.gov (right click; select "View Page Source"; use Ctrl+F to search for "javascript"). And the U.S. Courts' PACER privacy policy (which a user is not required to read or agree to before using the site) discloses that its website "use[s]s session cookies to identify users," without providing any more specifics about those cookies.[10] *See* https://pacer.uscourts.gov/privacy. Under the FAC's theory, the operators of those websites would be committing a crime any time anyone accessed those pages.

6. *The FAC fails to state a claim under the UCL.*

To state a claim under the UCL, Plaintiff must show (among other things) that Shopify Inc. engaged in an "unlawful," "fraudulent," or "unfair" business practice. Cal. Bus. & Prof. Code § 17200. Here, Plaintiff has failed to plead facts establishing any of those three.

a. <u>The FAC fails to state a claim for an "unlawful" practice.</u>

To state a UCL claim for an "unlawful" practice, a plaintiff must show a "violation[] of [an]other law[]." *Stripe*, 2021 WL 3191752, at *6. The FAC fails to do so. It lists five statutes as supposedly forming the basis for Plaintiff's claim: (1) the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 635 and 637; (2) the California Online Privacy Protection Act of 2003 ("CalOPPA"), Cal. Bus. & Prof. Code § 22575 *et seq.*; (3) the California Consumer Privacy Act of 2018 ("CCPA"), Cal. Bus. & Prof. Code § 1427 *et seq*; (4) Cal. Civ. Code § 3344; and (5) the California Computer Data Access and Fraud Act, Cal. Penal Code § 502. FAC ¶ 130.

As explained above and below, the FAC has not pled facts showing a violation of either (1) CIPA, (4) Cal. Civ. Code § 3344, or (5) Section 502. *See supra* §§ IV.C.2-3, IV.C.5; *infra* IV.C.7. Accordingly, none of those can serve as a basis for a UCL unfairness claim. Nor, as the *Stripe* Court explained, can the CCPA: "[T]he CCPA has no private right of action and on its face states that consumers may not use the CCPA as a basis for a private right of action under any statute."

[10] The PACER website also, of course, collects payment information when a user pays their bills—and presumably passes it on to a payment processor when the user pays by credit card.

Stripe, 2021 WL 3191752, at *7; *see also* Cal. Civ. Code § 1798.150(c) ("Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law.").

That leaves only CalOPPA. But, as in *Stripe*, "the complaint does an inadequate job of explaining the specific violation of th[at] statute," so it cannot serve as the basis for an "unlawful" practice claim under the UCL. 2021 WL 3191752, at *7 (dismissing UCL "unlawful" claim based on CalOPPA). In any event, the FAC has not pled and cannot plead a violation of CalOPPA, which exists where an "operator fails to post its policy within 30 days after being notified of noncompliance." Cal. Bus. & Prof. Code § 22575. The FAC nowhere alleges that Shopify Inc. was *ever* formally "notified of noncompliance," much less that it failed to post a privacy policy more than "30 days after" receiving such notice. *See id.*

b. <u>The FAC fails to state a claim for a "fraudulent" practice.</u>

"Claims stated under the fraud prong of the UCL are subject to the particularity requirements of Federal Rule of Civil Procedure 9(b)," meaning that the FAC "must state with particularity the circumstances constituting fraud or mistake," including "an account of the time, place, and specific content of the false representations at issue." *Stripe*, 2021 WL 3191752, at *7. Where, as here, a "fraudulent" UCL claim is based on a defendant's omission, the plaintiff must allege that the defendant had a duty to disclose the omitted fact. *See id.*; *see also Berryman v. Merit Prop. Mgmt., Inc.*, 152 Cal. App. 4th 1544, 1557 (2007) ("Absent a duty to disclose, the failure to do so does not support a claim under the fraudulent prong of the UCL.").

The FAC fails to satisfy either requirement, as it fails to state with the requisite particularly facts showing that Shopify Inc. (1) owed Plaintiff a duty to disclose its data collection practices; or (2) made any fraudulent or deceptive statements or omissions in breach of that specific duty. Indeed, the FAC's allegations going to the UCL "fraudulent" practice claim are near verbatim copies of those in the *Stripe* FAC (also filed by Plaintiff's counsel), *compare* FAC ¶¶ 127-128, *with Silver v. Stripe Inc.*, No. 20-cv-8196 (N.D. Cal. filed May 11, 2021), ECF No. 1 ¶¶ 203-204, which the *Stripe* Court held to be deficient on both of these grounds. *See* 2021 WL 3191752, at *7.

That decision was correct. California law recognizes only four circumstances in which an obligation to disclose may arise: "(1) when the defendant is in a fiduciary relationship with the plaintiff; (2) when the defendant had exclusive knowledge of material facts not known to the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; and (4) when the defendant makes partial representations but also suppresses some material facts." *Terpin v. AT&T Mobility, LLC*, 2020 WL 5369410, at *3 (C.D. Cal. 2020) (quoting *LiMandri v. Judkins*, 52 Cal. App. 4th 326, 336 (1997)). Rather than pleading specific facts to establish one of those four circumstances, the FAC only parrots those legal elements then adds the conclusory allegation that "Shopify [Inc.] owed the Class members a duty to disclose these facts because they were exclusively known and/or accessible to Shopify [Inc.], who had superior knowledge of its activities with respect to the private information of the Class members; [and] because Shopify [Inc.] actively concealed the facts." FAC ¶ 128. That is insufficient to survive a Rule 12(b)(6) motion. *See Iqbal*, 556 U.S. at 678 ("Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice."). This Court should not reach a different outcome here. Plaintiff's UCL claim for a "fraudulent" practice should be dismissed.

c. <u>The FAC fails to state a claim for an "unfair" practice.</u>

To state a claim for an "unfair" practice under the UCL, a plaintiff must plead facts showing that the challenged conduct violates a "public policy" that is "tethered" to a specific constitutional, statutory, or regulatory provision, or that the harm from the challenged conduct outweighs "the utility of the defendant's practice." *Stripe*, 2021 WL 3191752, at *8. Here, all the FAC has to say on that score is that "Shopify [Inc.] engaged in conduct that is unfair and unconscionable because its activities with respect to Class members' Private Information offends public policy, is immoral unethical, oppressive, outrageous, unscrupulous, and substantially injurious, and has caused substantial harm that greatly outweighs any possible utility from the conduct." FAC ¶ 133. But once again, that kind of "[t]hreadbare recital[] of the elements of a cause of action, supported by mere conclusory statements, do[es] not suffice," *Iqbal*, 556 U.S. at 678. Moreover, the FAC is simply wrong to say that Shopify Inc.'s conduct here was "immoral unethical, oppressive, outrageous, unscrupulous, and substantially injurious," FAC ¶ 133; to the contrary, it is nothing more than "routine commercial behavior." *See supra* § IV.C.4. Nor are there any facts to conclude that any of Shopify Inc.'s behaviors cause "substantial harm that greatly outweighs any possible utility." FAC ¶ 133. Rather, as the FAC admits, this routine commercial behavior enables Shopify Inc. to facilitate "over one million websites" that allow the same number of small- to medium-sized businesses to sell their products online. FAC ¶ 35. Plaintiff's claim that Shopify Inc.'s behavior is an "unfair" practice under the UCL should thus be dismissed.

7. *The FAC fails to state a claim for right of publicity.*

To state a claim for invasion of the right of publicity, a Plaintiff must plead facts showing, *inter alia*, that the defendant used his "name or likeness"—i.e., visual image," *White v. Samsung Elecs. Am., Inc.*, 971 F.2d 1395, 1397 (9th Cir. 1992)—for a prohibited purpose. *Gionfriddo*, 94 Cal. App. 4th at 409 (common law); Cal. Civ. Code § 3344(a) (statutory claim). But the FAC's assertions about Shopify Inc.'s supposed use of Plaintiff's "name and likeness"—specifically that it used that data "in the form of its risk profiles," FAC ¶ 153; *see also id.* ¶ 141—are not only conclusory, *see Iqbal*, 556 U.S. at 678 ("Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice."), but also contradicted by other allegations. For instance, FAC ¶ 36 purports to list the "information in the user profiles" that Shopify Inc. makes "available to its merchant customers"—but none of the information listed in that paragraph includes either a customer's name or visual image (likeness). Nor are there any factual allegations anywhere else in the FAC that support the notion that Shopify Inc. markets or otherwise uses Plaintiff's (or anyone else's) name or likeness. Because the FAC includes no non-conclusory allegations that establish this basic, and essential, element, it fails to state a right-of-publicity claim under either the statute or common law.

V. CONCLUSION

Shopify Inc. respectfully requests that the Court dismiss the FAC.

Dated: December 8, 2021

Respectfully Submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

By: */s/ Jacob M. Heath*
JACOB M. HEATH
THOMAS FU
Attorneys for Defendants
Shopify (USA), Inc. and Shopify Inc.